FORM PTO-1390 (REV 12-29-99)

U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: 0745/61002/NHZ

U.S. APPLICATION NO. (If known, see 37 CFR 1 5): 09/462616

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/DE98/01922	10 July 1998	10 July 1997

TITLE OF INVENTION: METHOD AND DEVICE FOR THE MUTUAL AUTHENTICATION OF COMPONENTS IN A NETWORK USING THE CHALLENGE-RESPONSE METHOD

APPLICANT(S) FOR DO/EO/US: Gunter MARINGER, Walter MOHRS and Edith PERNICE

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. [ ] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. [X] This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. [X] A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. [ ] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [ ] is transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] has been transmitted by the International Bureau.
   c. [ ] is not required, as the application was filed in the United States Receiving Of fice (RO/US).
6. [ ] A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. [ ] Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] have been transmitted by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [ ] have not been made and will not be made.
8. [ ] A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 3 71(c)(3)).
9. [X] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)), unexecuted.
10. [ ] A translation of the annexes to the International Preliminary Examination Repor t under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern document(s) or information included:

11. [ ] An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. [ ] An assignment document for recording. A separate cover sheet in compliance wit h 37 CFR 3.28 and 3.31 is included.
13. [ ] A FIRST preliminary amendment.
    [ ] A SECOND or SUBSEQUENT preliminary amendment.
14. [ ] A substitute specification.
15. [ ] A change of power of attorney and/or address letter.
16. [X] Other items or information: A copy of the International Application as published, including International Search Report and translation thereof, Express Mail Certificate of Mailing dated January 10, 2000, bearing Label No. EJ946 965 434US.

U.S. APPLICATION NO. (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
09/462616	PCT/DE98/01922	0745/61002/NHZ

17. [X] The following fees are submitted:	CALCULATIONS PTO USE ONLY	
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$970.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO **$840.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$690.00**		
International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$670.00**		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) **$96.00**		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 970.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$ 0	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	14 - 20 =	0	X **$18.00**	$0	
Independent claims	- 3 =		X **$78.00**	$ 0	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$260.00**	$ 0	
TOTAL OF ABOVE CALCULATIONS =				$970.00	
Reduction of 1/2 for filing by small entity, if applicable. A Small Entity Statement must also by filed (Note 37 CFR 1.9, 1.27, 1.28).				$	
SUBTOTAL =				$	
Processing fee of **$130.00** for furnishing the English translation later than [ ]20 [ ]30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$	
TOTAL NATIONAL FEE =				$	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$	
TOTAL FEES ENCLOSED =				$970.00	
				Amount to be refunded:	$
				charged:	$

a. [X] A check in the amount of $970.00 to cover the above fees is enclosed.

b. [ ] Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. [X] The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 03-3125. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Norman H. Zivin
COOPER & DUNHAM LLP
1185 Avenue of the Americas
New York, New York 10036

SIGNATURE:

Norman H. Zivin
NAME

25,385
REGISTRATION NUMBER

Article 34 amdt

Method and apparatus for mutual authentication of components in a network using the challenge-response method

The invention relates to a method and an apparatus for mutual authentication of components in a network using the challenge-response method, as claimed in the preamble of claim 1. In particular, the invention relates to mutual authentication of a terminal, preferably a mobile station, with the network, and vice versa. The following text uses the term "mobile station"; this should not be regarded as a limitation. This term is intended to cover all possible terminals, including stationary terminals, such as individual users of a computer in a wire-based system.

Authentication is used to check the authenticity of the component to be authenticated.

The prior art is the so-called challenge-response method: in this method, a random number (challenge) is sent by the authenticating component (N = network) to the component (M = mobile station) to be authenticated and is converted into a response using an algorithm (A) and a secret key K which is known to both components. The expected response is calculated in the network N using the same key K and the same algorithm A; a match between the response sent back by M and the response calculated in N proves the authenticity of M.

Article 34 Amend't

Mutual authentication is achieved according to the prior art by the above sequence being carried out with the opposite

AMENDED SHEET

role distribution. Such bidirectional authentication is described, for example, in EP-A-0 447 380.

Accordingly, in the known challenge-response method, the fixed network passes a challenge to the mobile station M, and the

mobile station M answers with a response which has been calculated by using a computation method which is implemented in the mobile station and which includes a secret key K. This key K is unique. This means that only this mobile station can respond in the way expected of it, provided it is authenticated as being "authentic". No other mobile station (M) can simulate this key.

A disadvantage of the previous method is that the entire authentication method can be verified only and exclusively in the AUC (authentication center), that is to say, in practice, in the computation center.

Specifically, for security reasons, it has been found to be advantageous in system architectures to control A and K at a central point (in the authentication center = AUC), with the authenticating point N (which carries out the authenticity check) having transmitted to it in advance only challenge/response pairs (possibly a number of them as a stockpile) for the purpose of authentication.

The challenge/response pairs transmitted from the AUC to the network (on request from the network in the form of a so-called "duplet request") are thus already to a large extent calculated in advance "as a stockpile" and, when the response arrives from the mobile station M during the authentication

process, the two responses are compared. If they match, this thus ends the authentication method for the mobile station M with the network N.

The known methods from the prior art accordingly provide for the mobile stations to authenticate themselves with the network. This results in a risk of the network

being simulated by unauthorized persons and thus of the relevant mobile station M being "spoofed by" the simulated network, with a mirror-image of the mobile station M being created in the process, but in this case for the "right" network N. In this unallowed situation, the M would authenticate itself with the simulated network N, thus allowing the unauthorized operator on the simulated network to call up non-public data from this mobile station M.

As one example, the GSM network should be mentioned which, at the moment, carries out only single-ended authentication (M authenticates itself with N). The TETRA Standard which is also known allows double-ended authentication.

The method is explained in the following text in order to provide a better description of the terms "Challenge 1, Response 1 and Challenge 2, Response 2" used later:

The Challenge 1 is used to authenticate the mobile station M with the network N. As soon as this authentication has been successfully completed, the mobile station M requests reverse authentication, such that a check is now carried out as to whether the present network N is also really the authorized network and not a network being simulated in an unallowed manner. The aim is thus to authenticate the network N with the mobile station M. In this case, the mobile station M

sends a Challenge 2 to the network, which passes the Challenge 2 on to the AUC where the Response 2 is calculated from it, and this is in turn sent to the network N, which passes the Response 2 to the mobile station. If the mobile station finds that the Response 2 which it has itself calculated matches the received Response 2, the authentication process is thus successfully ended. This authentication pair is referred to as Challenge 2/Response 2.

A disadvantage of mutual authentication in such system architectures is that the challenge sent by M cannot be converted into the response in N, but only in the AUC which, in some circumstances, leads to considerable time delays between the N-AUC-N data transfer and the on-line computation operation in the AUC.

The invention is based on the object of improving the known method for authentication of components in a network, in particular in a GSM network, such that this method is considerably speeded up.

In order to achieve the stated object, the method is distinguished by the fact that the Response 1 sent back by the mobile station M is simultaneously used by the network N as the Challenge 2, and this has the advantage that the Response 2 (as the response to the Challenge 2) is also calculated and transmitted by the AUC at the same time as the abovementioned challenge/response pairs. This avoids the time delay which would occur if N had to supply the Response 2 only after the Challenge 2 had arrived at the AUC.

The invention thus provides that, in order to identify the authenticity of the network N, the mobile station no longer produces a Challenge 2 internally and sends it to the network but, by equating the Response 1 to the Challenge 2, a mutual

match between M and N already exists via the expected Challenge 2. The network can thus produce a Response 2 at this stage and send it to the mobile station, which compares this Response 2 with the value it has itself calculated and, if they match, recognizes the network as being "authentic".

The important factor in this case is thus that the Response 1 sent from the mobile station to the network is at the same time used as the Challenge 2 from this mobile station, but which the mobile station no longer needs to send into the network, and waits for the Response 2 of the network. Specifically, the network already knows the Challenge 2 from the mobile station, since the Response 2 has already been calculated internally. The network can thus calculate the Response 2 at this stage.

According to the invention, the mutual authentication of the mobile station with the network and, after this, the authentication of the network with the mobile station are no longer carried out immediately successively in time, with a relatively high time penalty, but the two authentication tests are now interleaved with one another in time.

Complete data transmission of a test number (Challenge 2) is thus avoided since, according to the invention, the Challenge 2 can be saved and need no longer be transmitted. The separate transmission of the Response 2 by the network is saved due to the fact that the network sends the Response 2 to the mobile station at the same time that the Challenge 1 is sent. This is justified by the fact that the network already knows in advance what the Challenge 2 from the mobile station will be, that is to say the network can thus also

send the Response 2 to the mobile station immediately. The network thus transmits the data pair Challenge 1/Response 2 to the mobile station in a single data transmission. This means that the mobile station can identify the authenticity of N even before M has authenticated itself with N.

There are two different configurations in this case:

In a first embodiment, the network transmits the Challenge 1 to the mobile station. The mobile station M answers with the Response 1. Once a large number of triplet data packets (triplet = Challenge 1/Response 1/Response 2) have been transmitted in advance from the AUC to the network, the network N also knows the Response 1 of the mobile station M in advance. However, since it knows the Response 1, it also knows the Challenge 2. The mobile station now no longer sends the Challenge 2 to the network, but the network answers the Response 1 from M with the Response 2. However, only the "real" network has this knowledge; a simulated, unallowed network does not have this knowledge; the network N has thus authenticated itself with the mobile station by the transmission of a single data packet (Challenge 1/ Response 2), saving the transmission of the second data packet (Challenge 2).

In this case, it is advantageous that the Response 2 is a function of the Response 1. This means that the Response 2 can be calculated from the Response 1 = Challenge 2, provided the functional relationship is known. According to the prior art, the Response 2 was a function of the Challenge 2. According to the invention, the Challenge 2 need no longer be transmitted since Challenge 2 = Response 1 and is a function of Challenge 1.

In the end, making the Response 1 equivalent to the Challenge 2 means that the Response 2 is also a function of the Challenge 1.

Accordingly, in the first refinement, the Challenge 1 and the Response 2 are sent to the mobile station M immediately successively in time.

A second refinement provides for the Challenge 1 and Response 2 to be sent jointly to the mobile station M, as a data packet.
The mobile station answers this with the Response 1, and the network now compares the Response 1 with the expected value of Response 1, while the mobile station compares the Response 2 with the internally calculated value of the Response 2.

In known systems (for example in the GSM network), the length of the response (32 bits) is shorter than the challenge random number (128 bits). In order to allow the response to be used at the same time as a challenge for authentication of N with M using the same algorithm A, it is necessary to increase the length of Response 1 to the length of 128 bits expected by the algorithm A.
This could be achieved by quadruple concatenation of Response 1 (4 × 32 bits = 128 bits) or by filling out 128 bits in a previously defined manner (on a subscriber-specific basis or independently of the subscriber).

Proposals for the subscriber-specific filling-out process are:

1. Use of the complete computation result for the Response 1 before it has been shortened to 32 bits for transmission to the other station,

2. Filling out with defined bits from the K_i which is known in the M and AUC.

The advantage of both embodiments over the prior art is thus that the data traffic between the network and the mobile station on the one hand, as well as the data traffic between the network and the AUC is simplified, and thus speeded up. According to the prior art, four messages have to be sent backward and forward between the network and the mobile station M,

namely the Challenge 1, Response 1, Challenge 2 and Response 2.
Furthermore, the network must first transmit the Challenge 2 to the AUC, which must calculate the Response 2 and pass it to the network, and this is associated with a further time penalty.

According to the invention, time-consuming on-line interrogation from the network to the AUC is avoided. This is achieved in that the data packets required for this purpose from the AUC are called up even before the actual data traffic for authentication between the network and mobile station, and are buffer-stored for subsequent use in the network.

Such data packets (triplets) can be called up by the network from the AUC even well in advance (for example hours or days in advance). A common feature of both configurations in this case is that the Response 1 is used as the Challenge 2, and it is thus possible to dispense with the actual transmission of the Challenge 2.

A number of preferred exemplary embodiments will now be described in more detail with reference to the drawings. In this case, further features of the invention will become evident from the drawing and its description. In the drawing:

Fig. 1 shows, schematically, an authentication method according to the prior art,

Fig. 2 shows a first embodiment for authentication according to the invention,

Fig. 3 shows a second embodiment for authentication according to the invention.

In the configuration shown in Fig. 1, the network N first of all requests data sets as duplet packets (duplet request) from the AUC.

These duplet packets contain data sets for the Challenge 1/ Response 1. As soon as a mobile station M now wishes to authenticate itself with the network N, N first of all sends the data set Challenge 1 to M, which answers with the Response 1. If N finds that the two data sets match, the "authenticity" of M with N is thus proven. Conversely, M now requests the authenticity test of N by M sending to N a Challenge 2 which N passes on to the AUC where the required Response 2 is calculated from this, which the AUC passes to N, which in turn sends this to M. M now compares the internally calculated Response 2 and the Response 2 received from N, and recognizes the authenticity of N if the two match.

As has already been mentioned in the introduction, this convoluted data interchange places a severe load on the traffic between M and N on the one hand, and N and AUC on the other hand, and it is thus subject to time delays.
This is where the first version of the new method as shown in Fig. 2 comes into play, which provides for N to request so-called triplet data sets in the form of Challenge 1/ Response 1/Response 2 from the AUC. In this case, the data set Response 2 is a defined function of the data set Response 1, and can be calculated by means of an algorithm. Such data sets are requested from the AUC a very long time before the handling of the data traffic from N with M and are

stored in the form of multiple data sets in N. This avoids the necessity for on-line data traffic between N and the AUC, as was required for the prior art shown in Fig. 1.

In order to authenticate M with N, N first of all sends the Challenge 1 to M, which M answers with the Response 1. Once N has identified the data set Challenge 2 which is sent from M to N in the prior art, it is sufficient for N to send only the data set Response 2 to M

for authentication with M. M has calculated the data set Response 2 internally and compares this with the Response 2 sent from N. If they match, the "authenticity" of N with M is thus proven.

In contrast to the method shown in Figure 2, the second embodiment of the method, shown in Figure 3, provides for N to send the data set Challenge 1/Response 2 to M immediately and once. As soon as M sends back the data set Response 1, both authentication of M with N and, conversely, of N with M, are thus achieved.

PCT/DE98/01922

Patent claims

1. A method for mutual authentication of components in a network using the challenge-response method, in which, in order to authenticate a terminal (M), in particular a mobile station, with the network, the network (N) uses a request to request from an authentication center (AUC) at least one data pair comprising a first random number (Challenge 1) and a first response (Response 1), and passes the first random number (Challenge 1) to the terminal (M) which uses an internally stored key (Ki) likewise to calculate from this the first response (Response 1) and sends this to the network (N), in which case, furthermore, the network (N) is authenticated with the terminal (M) in that the terminal sends a second random number (Challenge 2) to the network, to which the network responds with a second response (Response 2) calculated in the AUC,
wherein
the first response (Response 1) sent from the terminal (M) to the network (N) is at the same time used as the second random number (Challenge 2), in which case the network has already requested the second response (Response 2) from the AUC in advance, together with the

first random number and the first response, as part of a triplet data set (Challenge 1/Response 1/Response 2).

2. The method as claimed in claim 1, wherein the network interprets the first response (Response 1), which is sent back from the terminal (M), as the second random number (Challenge 2).

AMENDED SHEET

Article 34 Amd't

3. The method as claimed in claim 1 or 2, wherein the first random number (Challenge 1) and the first response (Response 2) are transmitted from the network (N) to the terminal (M) immediately successively in time.

4. The method as claimed in claim 1 or 2, wherein the data pair (Challenge 1/Response 2) is transmitted from the network (N) to the terminal (M) simultaneously, in the form of a single data set.

5. The method as claimed in one of claims 2, 3 or 4, wherein the network requests data sets from the authentication center (AUC) in the form of triplet data sets (Challenge 1/Response 1/Response 2).

6. The method as claimed in claim 5, wherein a plurality of triplet data sets are supplied from the AUC as a stockpile, in order to reduce the request frequency.

7. The method as claimed in claim 4 or 5, wherein, in order to use the first response (Response 1) of the terminal (M) as the second random number (Challenge 2) in order to authenticate the network with the terminal (M), the shorter length of the first response (Response 1) is filled out to make up the greater length of the second random number (Challenge 2).

AMENDED SHEET

Article 34 Amd't

8. The method as claimed in claim 7, wherein the filling-out process is carried out on a subscriber-specific basis, and wherein the complete length of the first response (Response 1) is shortened before transmission to the other station.

9. The method as claimed in claim 8, wherein the first response (Response 1) is filled out with defined bits from the

AMENDED SHEET

secret key (Ki) to make up the length of the second random number (Challenge 2).

10. The method as claimed in claim 8, wherein the second random number (Challenge) corresponds to the original first response (Response 1) before it was shortened.

11. The method as claimed in one of claims 1-10, wherein the network is a GSM network.

12. The method as claimed in one of claims 1-10, wherein the network is a wire-based network.

13. The method as claimed in claim 12, wherein the individual, mutually authenticating components in a wire-based network are different monitoring units of computers which authenticate themselves with a central computer, and vice versa.

14. The method as claimed in one of claims 1-13, wherein the AUC calculates the triplet data sets requested by the network and transmits these to the network off-line and independently of time, on request by the network, but in any case before the data interchange between the network and the terminal.

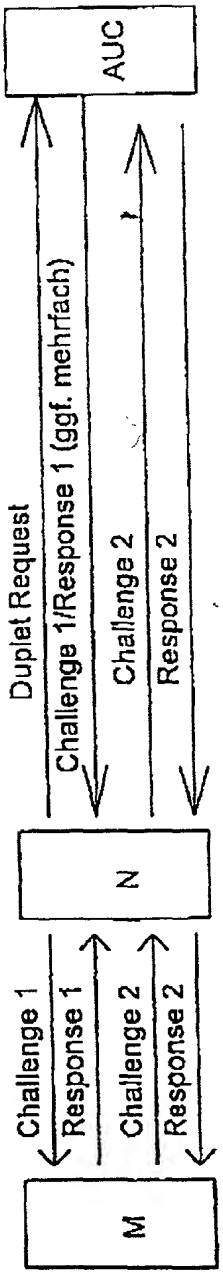

Fig. 1

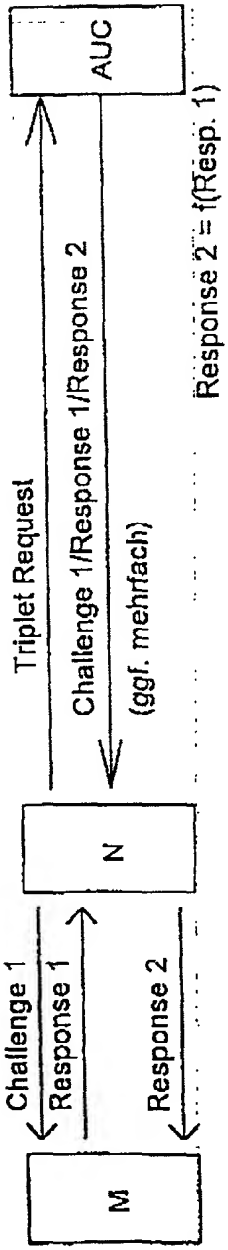

Fig. 2

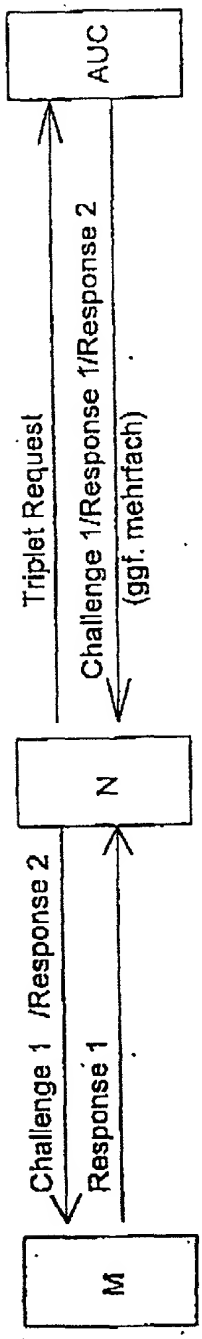

Fig. 3

Key to figures:

ggf. mehrfach = several times if necessary

Dkt. 61002

DECLARATION AND POWER OF ATTORNEY

As a below named inventors, We hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD AND DEVICE FOR THE MUTUAL AUTHENTICATION OF COMPONENTS IN A NETWORK USING THE CHALLENGE-RESPONSE METHOD

(Title of Invention)

the specification of which:
(check one)

_X_ *is attached hereto.*

___ *was filed on* ______________________

Application Serial No. ____________ ____________

and was amended ______________________
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information of which I am aware which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

Number	Country	Filing Date	Priority Claimed Yes	Priority Claimed No
197 29 611.4	GERMANY	July 10, 1997	Yes	
197 30 301.3	GERMANY	July 15, 1997	Yes	
PCT/DE98/01922	PCT	July 10, 1998	Yes	

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States Application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, Sections 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Application Serial No.	*Filing Date*	*Status*

And I hereby appoint ***Norman H. Zivin*** *(Reg. No. 25,385);* ***John P. White*** *(Reg. No. 28,678);* ***Ivan S. Kavrukov*** *(Reg. No. 25,161);* ***Christopher C. Dunham*** *(Reg. No. 22,031);* ***Robert D. Katz*** *(Reg. No. 30,141);* ***Peter J. Phillips*** *(Reg. No. 29,691); and* ***Wendy E. Miller*** *(Reg. No. 35,615 and each of them, all c/o Cooper & Dunham LLP of 1185 Avenue of the Americas, New York, New York 10036 (Tel. 212 278-0400), my attorneys, each with full power of substitution and revocation, to prosecute this application, to make alterations and amendments therein, to receive the patent, to transact all business in the Patent and Trademark Office connected herewith and to file any International Applications which are based thereon under the provisions of the Patent Cooperation Treaty.*

Please address all communications, and direct all telephone calls, regarding this application to:

Norman H. Zivin *Reg. No.* ***25,385***
Cooper & Dunham LLP
1185 Avenue of the Americas
New York, New York 10036
Tel. (212) 278-0400

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or first joint inventor Günter MARINGER

Inventor's signature [signature]

Citizenship Germany *Date of signature* 24.01.2000

Residence Troschelstr.8
53115 Bonn, GERMANY DEX

Post Office Address SAME AS RESIDENCE

2-10 Full name of joint inventor (if any) Walter MOHRS

Inventor's signature Walter Mohrs

Citizenship Germany Date of signature 23/2/2000

Residence Rosenhain 3

53123 Bonn, GERMANY DEX .

Post Office Address SAME AS RESIDENCE

1-11 Full name of joint inventor (if any) Frieder PERNICE, deceased, by his legal representative, Edith PERNICE

Inventor's signature Edith Pernice

Citizenship Germany Date of signature January, 20, 2000

Residence Schillerstr. 11

64846 Groß-Zimmern, GERMANY DEX

Post Office Address SAME AS RESIDENCE